PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

HYPERELLIPTIC CURVES OVER $\mathbb{F}_2$ OF EVERY 2-RANK WITHOUT EXTRA AUTOMORPHISMS

HUI JUNE ZHU

(Communicated by David E. Rohrlich)

Abstract. We prove that for any pair of integers $0 \leq r \leq g$ such that $g \geq 3$ or $r > 0$, there exists a (hyper)elliptic curve C over $\mathbb{F}_2$ of genus g and 2-rank r whose automorphism group consists of only identity and the (hyper)elliptic involution. As an application, we prove the existence of principally polarized abelian varieties (A, λ) over $\mathbb{F}_2$ of dimension g and 2-rank r such that $\mathrm{Aut}(A, \lambda) = \{\pm 1\}$.

1. Introduction

In this paper curves are smooth, projective, and geometrically integral algebraic varieties of dimension one defined over fields. Let k be a field and $\overline{k}$ its algebraic closure. If C is a curve over k, let $\mathrm{Aut}\, C$ denote the group of automorphisms of C defined over $\overline{k}$. Let $J(C)$ denote the Jacobian of C. Let $\mathrm{End}\, J(C)$ denote the endomorphism ring of $J(C)$ over $\overline{k}$. Let $\mathbb{F}_p$ be a finite field of p elements for some prime p. Let $\overline{\mathbb{F}}_p$ be its algebraic closure.

A supersingular curve C over $\mathbb{F}_p$ is a curve whose Jacobian is isogenous over $\overline{\mathbb{F}}_p$ to a product of supersingular elliptic curves. Hence a supersingular curve C is a cover of these supersingular elliptic curves. It has p-rank 0 but the converse is not true for $g \geq 3$. Supersingular curves are intimately connected to curves with large automorphism groups. For instance, in the seminal paper [1], the authors constructed supersingular curves over finite field of characteristic 2 by taking quotients of some families of (2-rank 0) curves over $\mathbb{F}_2$ with large automorphism groups. It is well-known that curves over fields of positive characteristic achieving maximal automorphism groups are all supersingular curves [13]. Is it a myth or truth that a curve over $\mathbb{F}_p$ of lower p-rank has larger automorphism groups in general?

In the moduli space of curves, the subset corresponding to the curves with trivial automorphism group is open (see [9, Introduction] or [2, Remark 10.6.24]). In a recent paper this fact was proved constructively [9] (see also [10][11]). It is desirable to understand how this subset stratifies by the p-rank of the curves.

Question 1. *Let p be a prime number. Given integers $g \geq 3$ and $0 \leq r \leq g$, is there a curve C over $\mathbb{F}_p$ of genus g and p-rank r such that $\mathrm{Aut}\, C = \{1\}$?*

Received by the editors March 28th, 2005.
2000 *Mathematics Subject Classification.* 11G10,14G15.
Key words and phrases. automorphism group, hyperelliptic curve.

There is not any constructive way to obtain curves over $\mathbb{F}_p$ of prescribed genus and p-rank, so we do not know the answer to this question.

On the other hand, for every prime p and positive integer g, Poonen [10] has constructed (hyper)elliptic curves C over $\mathbb{F}_p$ of genus g with $\operatorname{Aut} C = \{1, \iota\}$, where ι is the unique (hyper)elliptic involution of C. Automorphisms other than these two are referred as *extra* automorphisms.

If $g = 1$, it is well-known that for every prime p a supersingular elliptic curve (i.e., with zero p-rank) over $\mathbb{F}_p$ has extra automorphisms, while there exist ordinary elliptic curves (i.e., with non-zero p-rank) over $\mathbb{F}_p$ with $\operatorname{Aut} C = \{1, \iota\}$. (See [12, Chapter III].)

Every curve over $\mathbb{F}_2$ of genus 2 and 2-rank 0 can be written in the form $y^2 + y = x(x^4 + a_1 x^2 + a_0 x)$ for $a_0, a_1 \in \mathbb{F}_2$, hence has extra automorphisms. It is easy to check this fact by hand. In fact, every curve of the form $y^2 + y = x(\sum_{i=0}^{n} a_i x^{2^i})$ for some integer n and $a_i \in \mathbb{F}_2$ has extra automorphisms (see [1]).

Question 2. *Let p be a prime number. Given integers $g \geq 1$ and $0 \leq r \leq g$, is there a (hyper)elliptic curve C over $\mathbb{F}_p$ of genus g and p-rank r without extra automorphism?*

The present paper gives a complete answer to this question for the case $p = 2$. We hope this provides evidence for more general theorem or conjecture in the future.

Theorem 3. *For any integers $0 \leq r \leq g$ such that $g \geq 3$ or $r > 0$, there exists a (hyper)elliptic curve C over $\mathbb{F}_2$ of genus g and 2-rank r such that* $\operatorname{Aut}(C) = \{1, \iota\}$ *where ι is the unique (hyper)elliptic involution of C.*

The proof of the theorem, divided in two parts, is presented in the next two sections. This theorem has the following application. For an abelian variety A with polarization λ defined over $\mathbb{F}_2$ let $\operatorname{Aut}(A, \lambda)$ denote the group of automorphisms of A over $\overline{\mathbb{F}}_2$ respecting the polarization. The corollary below follows immediately from the theorem by applying the Torelli's theorem [6, Theorem 12.1]. Detailed discussion upon related results can be found in the Introduction of [10].

Corollary 4. *For any integers $0 \leq r \leq g$ such that $g \geq 3$ or $r > 0$, there exists a g-dimensional principally polarized abelian variety (A, λ) over $\mathbb{F}_2$ of 2-rank r such that* $\operatorname{Aut}(A, \lambda) = \{\pm 1\}$.

Finally we remark that these above two questions will be resolved if we know what algebras can become $\operatorname{End} J(C)$ for curves C over $\mathbb{F}_p$ of prescribed genus (see [8, Question (8.6)]) and p-rank. By [7] (see also [14]), one knows that for every $g \geq 1$ there exists a hyperelliptic curve C of any genus $g \geq 1$ with $\operatorname{End} J(C) = \mathbb{Z}$. However, this does not hold for curves over finite fields, in which case we have $\operatorname{End} J(C)$ strictly contains $\mathbb{Z}$.

2. Construction for $r > 0$

Suppose $g \geq 2$ and $r \leq g$ are two positive integers. Let $q(x)$ be a polynomial in $\mathbb{F}_2[x]$ of degree $< 2g + 1 - r$ (resp. $= 2g + 1 - r$) with r (resp. $r + 1$) distinct roots and, let $f(x)$ be a polynomial in $\mathbb{F}_2[x]$ of degree $2g + 1 - r$ (resp. $\leq 2g + 1 - r$), such that $f(x)$ and $q(x)$ has no common roots. Let C be the hyperelliptic curve over $\mathbb{F}_2$ defined by the affine equation

$$C : y^2 + y = \frac{f(x)}{q(x)}. \tag{1}$$

Then the curve C over $\mathbb{F}_2$ is of genus g by the Riemann-Hurwitz formula and of 2-rank r by the Deuring-Shafarevich formula in (2), which we shall explain immediately (see details in [4] or [5]). Let k be an algebraically closed field of characteristic p. Let $\pi : X \to Y$ be a finite Galois covering of curves over k whose Galois group G is a p-group. Let r_X and r_Y denote the p-ranks of X and Y, respectively. Let $Q_1, \cdots, Q_n$ be the set of ramification points on Y with respect to π. For each point Q_i let p^{e_i} (here $e_i \geq 1$) be its ramification index. Then

$$r_X - 1 = \#G \cdot (r_Y - 1 + \sum_{i=1}^{n}(1 - p^{-e_i})). \tag{2}$$

Let D be the ramification divisor of the canonical double cover $C \to \mathbb{P}^1$. Write $q := \prod_{i=1}^{r}(x - \alpha_i)^{b_i}$ (resp. $q := \prod_{i=1}^{r+1}(x - \alpha_i)^{b_i}$) for distinct $\alpha_i \in \overline{\mathbb{F}}_2$ and $b_i \in \mathbb{Z}_{>0}$. The set $\mathcal{S}$ of ramification points consists of those points P_{α_i} corresponding to the zeroes of q and possibly the point P_∞ at infinity. We have

$$D = \begin{cases} (2g + 2 - \deg(q) - r)P_\infty + \sum_{i=1}^{r}(b_i + 1)P_{\alpha_i} & \text{and respectively} \\ \sum_{i=1}^{r+1}(b_i + 1)P_{\alpha_i} \end{cases} \tag{3}$$

Every automorphism of C gives rise to an automorphism of $\mathbb{P}^1$ preserving D under the canonical double cover $C \to \mathbb{P}^1$. To construct curves C without extra automorphisms, it suffices to find monic polynomials f and q in $\mathbb{F}_2[x]$ such that every automorphism of $\mathbb{P}^1$ preserving D is the identity map on $\mathbb{P}^1$.

Our construction below follows the following idea: for every pair of integers $0 < r \leq g$, we shall construct polynomials q such that q has r (or $r + 1$ resp.) distinct roots and of degree $< 2g + 1 - r$ (or $2g + 1 - r$, resp.) in $\mathbb{F}_2[x]$. We always let f be any polynomial in $\mathbb{F}_2[x]$ of degree $2g + 1 - r$ (or $\leq 2g + 1 - r$, resp.) which has no common roots with q. We remark that we shall use the construction that q has r distinct roots except in *Case 5* and *Case 6*.

In the construction below we use the notation f_n for a n-th degree irreducible polynomial in $\mathbb{F}_2[x]$. It is a basic fact in algebra that f_n exists for every positive integer n (see [3, Chapter V]). For example, $f_2 = x^2 + x + 1$ and $f_3 = x^3 + x^2 + 1$ or $x^3 + x + 1$. For any f_3 of our choice, we denote by $\beta_1, \beta_2, \beta_3$ its roots in $\overline{\mathbb{F}}_2$ in an order such that $\beta_1^2 = \beta_2$.

Case 1. Suppose $r \geq 8$:

Let $q = f_3 f_{r-3}$ if $3 \nmid r$ and $q = x f_3 f_{r-4}$ otherwise.

Let σ be an automorphism of $\mathbb{P}^1$ which acts as a 3-cycle on the three roots of f_3 in $\overline{\mathbb{F}}_2$. Since 3 points determines an automorphism of $\mathbb{P}^1$, σ is defined over the field k generated by roots of f_3 over $\mathbb{F}_2$. Hence, $\sigma(P_\infty)$ corresponds to a point in k.

Let $\mathbb{F}$ denote the composition of all finite extensions of $\mathbb{F}_2$ of degrees coprime to 3. There are exactly $r - 2$ distinct $\mathbb{F}$-rational points in the set of ramification points $\mathcal{S}$. Suppose λ is a non-trivial automorphism of $\mathbb{P}^1$ preserving D. Then λ must map at least $(r - 2) - 3 \geq 3$ of these $\mathbb{F}$-rational points to other $\mathbb{F}$-rational points of $\mathcal{S}$. But λ is determined by its values at 3 points, so λ must be defined over $\mathbb{F}$. In particular, λ preserves the set of 3 non-$\mathbb{F}$-rational points of $\mathcal{S}$, the roots of f_3. If λ fixes any one of them, as they are Galois conjugates over $\mathbb{F}$, then λ would fix them all, hence λ would be trivial. So λ acts as a 3-cycle, and after replacing λ by λ^{-1} if necessary, we may assume $\lambda = \sigma$. Since λ permutes the roots of f_3, it fixes its coefficients, hence λ fixes 0 and 1. So $\lambda(P_\infty) \neq P_\infty$ and $\lambda(P_\infty) \neq P_1$. But

D is preserved, so λ maps P_∞ to a root of f_{r-3} (or f_{r-4}), which lies in $\mathbb{F}$ and does not lie in k. This contradicts our assumption above about σ.

Case 2. Suppose $r = 1$ and $g \geq 2$, or $r = 2$ and $g \geq 4$:

For $r = 1$ and $g \geq 2$, let $q = x$.

Then the ramification divisor is $D = 2gP_\infty + 2P_0$. Since $g \geq 2$ every automorphism of $\mathbb{P}^1$ preserving D fixes ∞ and 0, hence it is of the form $x \mapsto cx$ for some non-zero $c \in \overline{\mathbb{F}}_2$. A simple computation shows that $c = 1$. This resembles Case I in Section 2 of [10].

For $r = 2$ and $g \geq 4$, let $q = x^2(x+1)$.

Then $D = (2g-3)P_\infty + 3P_0 + 2P_1$. Every automorphism of $\mathbb{P}^1$ preserving D has three points $\infty, 0$ and 1 all fixed hence is identity.

Case 3. Suppose $r = 3$ and $g \geq 4$:

Let $q = f_3$.

Then $D = (2g-4)P_\infty + 2(P_{\beta_1} + P_{\beta_2} + P_{\beta_3})$. Let λ be a non-trivial automorphism of $\mathbb{P}^1$ that preserves D. By assumption $2g - 4 > 2$, so λ fixes P_∞ and λ permutes the roots of f_3. Thus λ fixes 0 and 1. But then it fixes all three points $0, 1$ and ∞, it must be identity. This leads to a contradiction.

These following three cases follow the same scheme, so we shall elaborate on Case 4 and only sketch the rest two cases.

Case 4. Suppose $r = 4$ and $g \geq 5$, or $r \geq 4$ and $g \geq r + 3$:

For $r = 4$ and $g \geq 5$, let $q = x^2 f_3$.

Then the ramification divisor is $D = (2g-7)P_\infty + 3P_0 + 2(P_{\beta_1} + P_{\beta_2} + P_{\beta_3})$. Let λ be a non-trivial automorphism of $\mathbb{P}^1$ which preserves D, then λ permutes the roots of f_3 hence it fixes 0 and 1. If fixes P_∞ and P_0 then it is identity. If λ swaps P_∞ and P_0, and it is of the form $\lambda(\alpha) = c/\alpha$ for some non-zero $c \in \overline{\mathbb{F}}_2$. It can be checked quickly that this map can not preserve the roots of f_3.

For $r \geq 4$ and $g \geq r + 3$, let $q = x^3(x+1)^2 f_{r-2}$.

Then $D = (2g - 2r - 1)P_\infty + 4P_0 + 3P_1 + 2\sum_{(f_{r-2})_0} P$. Since $2g - 2r - 1 \geq 5$ and $r - 2 \geq 2$, every automorphism of $\mathbb{P}^1$ preserving D has three points $\infty, 0$ and 1 all fixed hence is identity.

Case 5. Suppose $r = 5$ and $g \geq 5$:

Let $q = f_3(x+1)^{2g-9}(x^2+x+1)$. Let α_1, α_2 be roots of $x^2 + x + 1$ in $\overline{\mathbb{F}}_2$.

Then the ramification divisor is

$$D = 2(P_{\beta_1} + P_{\beta_2} + P_{\beta_3}) + (2g-8)P_1 + 2(P_{\alpha_1} + P_{\alpha_2}).$$

Label the roots of $\beta_1, \beta_2, \beta_3, 1, \alpha_1, \alpha_2$ by $1, 2, 3, 4, 5, 6$, respectively, such that the absolute Frobenius acts on $\mathcal{S}$ as the permutation $\sigma = (123)(56)$. Let H be the subgroup of the automorphism of $\mathbb{P}^1$ preserving D, which we may view as a faithful subgroup of S_6, since automorphisms are determined already by 3 values. Any automorphism of $\mathbb{P}^1$ which fixes α_1 and α_2 has to fix 1 so β_3 can not be mapped to 1. Therefore, $(12)(34) \notin H$. The group theoretical lemma below, due to Poonen (see [10, Lemma 3]), indicates that H is trivial.

Lemma 5. *Suppose H is a subgroup of S_6 such that*

(1) *Each non-trivial element of H has at most 2 fixed points;*

(2) *$\sigma H\sigma^{-1} \subset H$ for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_2/\mathbb{F}_2)$;*
(3) *The permutation $(12)(34)$ is not in H,*

Then $H = \{1\}$.

Case 6. Suppose $r = 6$ and $g \geq 7$:

Let $q = f_3(x+1)(x^2+x+1)x^{2g-11}$.
Then the ramification divisor is $D = 2(P_{\beta_1} + P_{\beta_2} + P_{\beta_3}) + 2P_1 + 2(P_{\alpha_1} + P_{\alpha_2}) + (2g-10)P_0$. Note that every automorphism of $\mathbb{P}^1$ preserving D fixes P_0. Then we apply the same argument as in *Case 5*.

Case 7. Suppose $r = 7$ and $g \geq 8$:

Let $q = f_3(x+1)(x^2+x+1)x^2$.
Then the ramification divisor is

$$D = 2(P_{\beta_1} + P_{\beta_2} + P_{\beta_3}) + 2P_1 + 2(P_{\alpha_1} + P_{\alpha_2}) + 3P_0 + (2g-13)P_\infty.$$

Let λ be a non-trivial automorphism of $\mathbb{P}^1$ preserving D. If λ fixes P_0 and P_∞ then we use the same argument as in *Case 5*. This is the case when $g \geq 9$. It remains to prove the case $g = 8$ and λ swaps P_0 and P_∞. Then $\lambda(\alpha) = c/\alpha$ for some non-zero $c \in \overline{\mathbb{F}}_2$. If λ fixes P_1 then it is defined over $\mathbb{F}_2$ hence it permutes the roots of f_3 and fixes P_0, contradiction. If λ swaps P_1 with one root of f_3, then it preserves the roots of f_3 also. If λ swaps P_1 with a root of f_2 then it permutes the roots of f_2. So it has to fixes P_1, which is absurd.

Case 8. Remaining cases:

For $g = r = 4, 6$, let $C : y^2 + y = x + \frac{1}{x(x^{r-1}+1)}$.
For $g = r = 3, 5, 7$, let $C : y^2 + y = x + \frac{1}{x^r+1}$.
For $g = 2, 3$ and $r = 2$, let $C : y^2 + y = x + \frac{1}{x^2+x+1}$ and $C : y^2 + y = x^3 + \frac{1}{x^2+x+1}$, respectively.

It is an elementary computation to show that these curves have no extra automorphisms.

3. Construction for $r = 0$

We still assume $g \geq 2$. In this section let C be a hyperelliptic curve defined by the affine equation

$$C : y^2 + y = f(x) \tag{4}$$

where $f(x)$ is a polynomial in $\mathbb{F}_2[x]$ of degree $2g+1$. This is the same as letting $q = 1$ in (1). So C is of genus g and 2-rank 0. We remark that every curve in (4) is isomorphic to a curve with only odd-degree terms in $f(x)$ because the base field is $\mathbb{F}_2$.

Any automorphism of C is of the form $x \mapsto ax + b$ and $y \mapsto cy + h(x)$ for some $a, b, c \in \overline{\mathbb{F}}_2$ and some polynomial $h(x)$ in $\overline{\mathbb{F}}_2[x]$ of $\deg(h) \leq g$. Let $\mathcal{H}$ be the set of polynomials $p(x)^2 + p(x)$ for all polynomial $p(x)$ in $\overline{\mathbb{F}}_2[x]$ of degree $\leq g$. It is easy to show that it is a $\overline{\mathbb{F}}_2$-vector space of dimension $g+1$. It follows that $c = a^{2g+1} = 1$ and $f(ax+b) + f(x) = h(x)^2 + h(x)$. That is

$$a^{2g+1} = 1 \quad \text{and} \quad f(ax+b) + f(x) \in \mathcal{H}. \tag{5}$$

Lemma 6. *Let $g = 4$ or $g \geq 7$. Let $p(x)$ be a polynomial in $\mathbb{F}_2[x]$ of degree $\leq 2g-6$. The hyperelliptic curve C defined by the affine equation*

$$C : y^2 + y = f(x) := x^{2g+1} + x^{2g-1} + x^{2g-3} + p(x)$$

has $\operatorname{Aut} C = \{1, \iota\}$ *if and only if either $g \not\equiv 2 \bmod 4$, or $g \equiv 2 \bmod 4$ and*

(i) *$g - 2$ is a 2-power and $p(x+1) + p(x) \notin \mathcal{H}$;*
(ii) *$g - 2$ is not a 2-power and*

$$p(x+1) + p(x) \notin \mathcal{H} + (x^4 + x^2 + 1)((x+1)^{2g-3} + x^{2g-3}) \neq \mathcal{H}.$$

Proof. Suppose $x \mapsto ax + b$ gives rise to a non-extra automorphism λ of C.

First we suppose $g \geq 7$. If $b = 0$ then (5) implies that $a = 1$ and so λ is not extra. Otherwise, since $\deg(f(ax+b)+f(x)) = 2g$, all odd-degree terms in $f(ax+b)+f(x)$ of degree $> g$ vanish. Because $2g - 5 > g$ by our assumption, the coefficients of x^{2g-1}, x^{2g-3} and x^{2g-5} are zero. That is,

$$\binom{2g+1}{2} b^2 + 1 + a^2 = 0 \tag{6}$$

$$\binom{2g+1}{4} b^4 + \binom{2g-1}{2} b^2 + 1 + a^4 = 0 \tag{7}$$

$$\binom{2g+1}{6} b^4 + \binom{2g-1}{4} b^2 + \binom{2g-3}{2} = 0 \tag{8}$$

Simplifying, we get respectively

$$g b^2 + 1 + a^2 = 0 \tag{9}$$

$$\frac{g(g-1)}{2} b^4 + (g-1) b^2 + 1 + a^4 = 0 \tag{10}$$

$$\frac{g(g-1)(g-2)}{2} b^4 + \frac{(g-1)(g-2)}{2} b^2 + g = 0. \tag{11}$$

Substitute (9) to (10) we get

$$\frac{g(g-1)}{2} b^4 + (g-1) b^2 + g^2 b^4 = 0;$$

and so

$$\frac{g(3g-1)}{2} b^2 + (g-1) = 0.$$

Thus $\frac{g(3g-1)}{2} = g - 1$ and $g \equiv 1, 2 \bmod 4$. But (11) implies $g \not\equiv 1 \bmod 4$.

From now on we assume $g \equiv 2 \bmod 4$. Under this condition we get $a = b = 1$ by (9) and (10). Once again, we use (5) to get

$$f(x+1) + f(x) = (p(x+1) + p(x)) + \gamma(x) \in \mathcal{H},$$

where $\gamma(x) = (x^4 + x^2 + 1)((x+1)^{2g-3} + x^{2g-3})$.

We claim that $\gamma(x) \in \mathcal{H}$ if and only if $g-2$ is a 2-power. Suppose $\gamma(x) \in \mathcal{H}$. We have $\deg(\gamma) = 2g$ and the its odd-degree terms are

$$\begin{array}{ll}
 & \binom{2g-3}{2}x^{2g-1} \\
+ & (\binom{2g-3}{2} + \binom{2g-3}{4})x^{2g-3} \\
+ & (\binom{2g-3}{2} + \binom{2g-3}{4} + \binom{2g-3}{6})x^{2g-5} \\
+ & (\binom{2g-3}{4} + \binom{2g-3}{6} + \binom{2g-3}{8})x^{2g-7} \\
+ & \cdots \\
+ & (\binom{2g-3}{2m-4} + \binom{2g-3}{2m-2} + \binom{2g-3}{2m})x^{2g-(2m-1)}
\end{array}$$

Set the odd-degree terms of degree $> g$ zero, and use the identity $\binom{2g-3}{2n} = \binom{g-2}{n}$ over $\mathbb{F}_2$ for all n, we have

$$\begin{array}{rcl}
\binom{g-2}{1} & = & 0 \\
\binom{g-2}{1} + \binom{g-2}{2} & = & 0 \\
\binom{g-2}{1} + \binom{g-2}{2} + \binom{g-2}{3} & = & 0 \\
\binom{g-2}{2} + \binom{g-2}{3} + \binom{g-2}{4} & = & 0 \\
 & \vdots & \\
\binom{g-2}{m-2} + \binom{g-2}{m-1} + \binom{g-2}{m} & = & 0
\end{array}$$

for $m < \frac{g+1}{2}$. But we already have $\binom{g-2}{1} = \binom{g-2}{2} = \binom{g-2}{3} = 0$, so this system of equations has a solution if and only if $\binom{g-2}{m} = 0$ for all $m \leq \frac{g}{2}$. That is, $g-2$ is a 2-power. This proved parts (i) and (ii).

When $g = 4$, we follow the same argument but only simpler. Namely, any non-trivial automorphism λ will lead to (9) and (10) and hence $g \equiv 1, 2 \bmod 4$. Contradiction. □

Case 9. Suppose $r = 0$ and $g = 4$ or $g \geq 7$:

Let $f(x) = x^{2g+1} + x^{2g-1} + x^{2g-3} + p(x)$, where $p(x)$ is any polynomial in $\mathbb{F}_2[x]$ of degree $\leq 2g-6$ such that $g \not\equiv 2 \bmod 4$, or $g \equiv 2 \bmod 4$ and

(i) if $g-2$ is a 2-power, then let $p = x^n + x^{n-2} +$ (lower-degree terms) where $n \equiv 3 \bmod 4$; or

(ii) if $g-2$ is not a 2-power, then let $p \in \mathcal{H}$.

We shall verify our construction above. If $g \not\equiv 2 \bmod 4$ it follows from Lemma 6. Suppose $g \equiv 2 \bmod 4$. It can be easily checked that part (i) implies $p(x+1)+p(x) \notin \mathcal{H}$ so it follows from part (i) of the same Lemma. In part (ii) $p \in \mathcal{H}$ implies that $p(x+1)+p(x) \in \mathcal{H}$. Since $g-2$ is not a 2-power, $\mathcal{H}+(x^4+x^2+1)((x+1)^{2g-3}+x^{2g-3})$

is a non-trivial coset of $\mathcal{H}$, hence is disjoint from $\mathcal{H}$. So part (ii) follows from part (ii) of the same Lemma again.

Case 10. Suppose $r = 0$ and $g = 6$:

Let $f = x^{2g+1} + x^{2g-3} + x^{2g-5} + p(x)$ where $p(x)$ is a polynomial in $\mathbb{F}_2[x]$ of degree $\leq 2g - 6$.

Suppose $x \mapsto ax + b$ gives rise to an automorphism λ of C. For any $g \equiv 2 \bmod 4$ we show that the only possible extra automorphism is the one given by a, b are both 3-rd roots of unity over $\mathbb{F}_2$. Apply (5) to coefficients of $x^{2g}, x^{2g-1}, x^{2g-3}, x^{2g-5}$, those are $a^{2g}b, 1 + a^{2g-3}(1 + b^4), 1 + a^{2g-5}$. If $b = 0$ then $a = 1$ so it is trivial. If $b \neq 0$ then $a = b + 1$ and $a^3 = 1$. If it is not trivial then a, b are 3-rd roots of unity.

When $g = 6$ we have $a^{2g-5} = a^7 = 1$ and $a^6 = 1$ so $a = 1$. This implies $b = 0$. So λ is trivial.

Case 11. Suppose $r = 0$ and $g = 3$ or 5:

Let $f = x^{2g+1} + x^{2g-3} + p(x)$ where $p(x)$ is a polynomial in $\mathbb{F}_2[x]$ of degree $2g - 5$. In fact, this construction works for every odd $g \geq 3$.

Suppose $x \mapsto ax + b$ gives rise to an automorphism λ of C. The coefficient of x^{2g} and x^{2g-1} in $f(ax + b) + f(x)$ are $a^{2g}b$ and $a^{2g-1}b$, respectively. At least one of them has to vanish by (5), so $b = 0$. This implies $a = 1$ by applying (5) again.

Acknowledgments. The author thanks R. Coleman and B. Poonen for valuable correspondences and remarks on draft of this paper. She is grateful to H. Lenstra for support and the Mathematisch Institute of Universiteit Leiden for its hospitality, where part of this work was done in 2000. Finally she thanks the referee for comments.

References

1. G. van der Geer and M. van der Vlugt, *Reed-Muller codes and supersingular curves.* I, Compositio Math. **84** (1992), 333–367.
2. N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc. Colloq. Publ. **45**, Amer. Math. Soc., Providence, RI, 1999.
3. S. Lang, *Algebra*, Third Edition, Addison-Wesley Publishing Company, 1993.
4. M. Madan, *On a theorem of M. Deuring and I.R. Shafarevich*, Manuscripta Math. **23** (1977), 91–102.
5. S. Nakajima, *Equivariant form of the Deuring-Shafarevich formula for Hasse-Witt invariants*, Math. Z. **190** (1985), 559–566.
6. J. Milne, *Jacobian varieties*, Arithmetic Geometry (Storrs, Conn., 1984), 167–212. Springer, New York, 1986.
7. S. Mori, *The endomorphism rings of some abelian varieties*, Japan. J. Math., **2**(1976), 109–130.
8. F. Oort, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, 469–502, Kinokuniya, Tokyo, 1988.
9. B. Poonen, *Varieties without extra automorphisms I: Curves*, Math. Res. Letters, **7** (2000), 67–76.
10. B. Poonen, *Varieties without extra automorphisms II: Hyperelliptic curves*, Math. Res. Letters **7** (2000), 77–82.
11. B. Poonen, *Varieties without extra automorphisms III: Hypersurfaces*, Finite Fields Appl. **11** (2005), no.2, 230–268.
12. J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag, 1986.
13. H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math.(Basel) **24** (1973), 527–544.

14. Y. Zarhin, *Hyperelliptic Jacobians without complex multiplication in positive characteristic*, Math. Res. Lett. **8** (2001), no.4, 429–435.

Department of Maths and Stats, McMaster University, Hamilton, ON L8S 4K1, CANADA

E-mail address: zhu@cal.berkeley.edu